Install Guide

for FortiAuthenticator-VM™ 1.0 MR3

Carl Windsor

Contents

Overview of FortiAuthenticator-VM

Welcome, and thank you for selecting Fortinet products to protect your network.

FortiAuthenticator-VM is a virtual appliance designed specifically to provide authentication services for multiple devices, including firewalls, SSL and IPSec VPNs, switches, routers and servers. FortiAuthenticator includes a RADIUS and LDAP server. Authentication servers are an important part of an enterprise network, access to protected network assets and tracking users' activities to comply with security policies.

A FortiAuthenticator is ***not*** a firewall; it requires a FortGate appliance to provide firewall-related services. Multiple FortiGate units can use a single FortiAuthenticator appliance for Fortinet Single Sign-On (FSSO) and other types of remote authentication, two-factor authentication, and FortiToken device management. This centralizes authentication and FortiToken maintenance.

FortiAuthenticator provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the FSSO Agent on a Windows AD network.

Whilst FortiAuthenticator is a hardened server ***it should be installed with adequate protection from the internet***. Management protocols should be configured on private networks and only the resources required exposed to the outside.

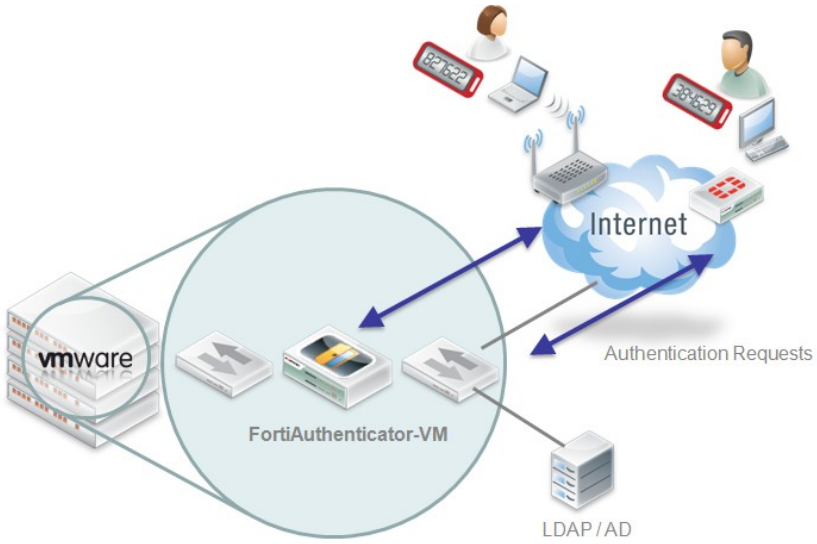
Caution: Failure to protect the FortiAuthenticator may result in compromised authentication databases.

Architecture

FortiAuthenticator-VM is a virtual appliance version of FortiAuthenticator. It is deployed in a virtual machine environment such as VMware vSphere or ESXi.

Once the virtual appliance is deployed and set up, you can manage FortiAuthenticator-VM via its web UI from a web browser on your management computer.

FortiAuthenticator-VM architecture



FortiAuthenticator-VM requires the following connectivity:

Inbound Management

Telnet	TCP 23 (Not recommended)
HTTP	TCP 80 (Not recommended)
HTTPS	TCP443
SSH	TCP 22

Outbound Management

DNSlookup	UDP 53
NTP	UDP 123
FortiGuard licensing	TCP 443 (required for initial token registration)
Log Export (FTP)	TCP 21

Inbound Authentication (dependent on services configured)

RADIUS Authentication	UDP 1813
RADIUS Accounting	UDP 1812
LDAP/LDAPS	TCP 389/636
OCSP	TCP 2560

Outbound Authentication (dependent on services configured)

LDAP/LDAPS	TCP 389/636
FSSO	TCP 8000

Licensing

FortiAuthenticator-VM licenses require a base license plus any additional user licenses that are required. Licenses are stackable, allowing on-the-fly upgrades with a license key

FortiAuthenticator-VM licenses

FAC-VM-Base	**Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU**
FAC-VM-100-UG	FortiAuthenticator-VM with 100-user license upgrade
FAC-VM-1000-UG	FortiAuthenticator-VM with 1000-user license upgrade
FAC-VM-10000-UG	FortiAuthenticator-VM with 10,000-user license upgrade
FAC-VM-100000-UG	FortiAuthenticator-VM with 100,000-user license upgrade

For example, to support 3,400 users, you would require:

1 x FC-VM-Base (includes 100-user license)
3 x FAC-VM-1000-UG
3 x FAC-VM-100-UG

FortiAuthenticator-VM support

Support is sold separately and is based on the total number of users being managed:

SKU	Description
FC1-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 – 500-Users)
FC2-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 1100-Users)
FC3-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 5100-Users)
FC4-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 10100-Users)
FC5-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 50100-Users)
FC6-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 100100-Users)

i.e. To support 3,400 users, you would require the FC3-10-0ACVM-248-02-12 1 year 24x7 FortiCare technical support contract.

FortiAuthenticator-VM Maximum Values

Further details on licensing sizing limitations can be found in Appendix A – Maximum Values

License file generation

When you place an order for FortiAuthenticator-VM, Fortinet emails a registration number to the recipient address you supplied on the order form. Enter that registration number on the Fortinet Technical Support web site to register your appliance with Technical Support and to obtain a license file.

https://support.fortinet.com/

The license file is required to permanently activate FortiAuthenticator-VM. For details, see Downloading the FortiAuthenticator-VM software & registering with Technical Support).

Evaluation

FortiAuthenticator-VM includes a free 2-user license that is fully functional. You do not need to manually upload the trial license. It is built-in.

An extended trial license for up to 100 users and up to 90 days is available. Please contact your account manager or Fortinet for more details.

Note: Technical support is ***not*** included with the 2 user free trial license included with FortiAuthenticator-VM. Please request an official trial license.

Scope

This document describes how to deploy a FortiAuthenticator virtual appliance disk image onto a virtualization server, and how to configure the virtual hardware settings of the virtual appliance. It assumes you have already successfully installed a virtualization server on the physical machine.

This document does ***not*** cover initial configuration of the virtual appliance itself, nor ongoing use and maintenance. After deploying the virtual appliance, for information on initial appliance configuration, see the *FortiAuthenticator Administration Guide*.

This document is intended for administrators, not end users. If you have a user account on a computer that accesses web sites through a FortiAuthenticator appliance, please contact your system administrator.

Conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at:

http://ietf.org/rfc/rfc1918.txt?number-1918

For example, even though a real network's Internet-facing IP address would be routable on the public Internet, in this document's examples, it would be shown as a non-Internet-routable IP such as 10.0.0.1, 192.168.0.1, or 172.16.0.1.

Cautions, notes, & tips

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Note: Presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.

Tip: Highlights useful additional information, often tailored to your workplace activity.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From *Minimum log level*, select *Notification*.

CLI input	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system settings`
	`comments : (null)`
	`opmode : nat`

Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>` `<BODY><H4>You must authenticate to use this service.</H4>`
Hyperlink	https://support.fortinet.com
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to *VPN* > *IPSEC* > *automatic Key (IKE)*.
Publication	For details, see the *FortiAuthenticator Administration Guide*.

Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Command syntax notation

Convention		Description

Square brackets `[ ]`		A non-required (optional) word or words. For example:
		`[verbose {1 | 2 | 3}]`
		indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:
		`verbose 3`

Curly braces `{ }`		A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
	Options delimited by vertical bars `|`	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

	Options delimited by spaces	Non-mutually exclusive options. For example:
		`{http https ping snmp ssh telnet}`
		indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
		`ping https ssh`
		Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:
		`ping https snmp ssh`
		If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Command syntax notation

Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>` — A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>` — An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>` — A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all e-mail addresses ending in `@example.com`. • `<xxx_fqdn>` — A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>` — An email address, such as `admin@mail.example.com`. • `<xxx_url>` — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`. • `<xxx_ipv4>` — An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>` — A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>` — A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>` — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`. • `<xxx_ipv6>` — A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>` — An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>` — An IPv6 address and netmask separated by a space. • `<xxxstr>` — A string of characters that is ***not*** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the *FortiProduct CLI Reference*.

Command syntax notation

	• `<xxx_int>` — An integer number that is ***not*** another data type, such as `15` for the number of minutes.

System requirements

Before you can install FortiAuthenticator-VM, you must first have virtual machine (VM) environment software (a hardware abstraction layer (HAL) that is sometimes called a hypervisor) on your server. FortiAuthenticator-VM is a virtual appliance that runs inside that environment.

Supported hypervisor versions include:

- VMware vSphere ESX 4.0/4.1
- VMware vSphere ESXi 4.0/4.1
- VMware vSphere Hypervisor 4.0/4.1/5.0

Tip: For best performance, install FortiAuthenticator-VM on a “bare metal” hypervisor, such as VMware ESXi. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host will have fewer computing resources available due to the host OS’s own overhead.

For installation instructions, see the documentation for your VM environment, such as:

- http://www.vmware.com/products/esxi
- http://www.vmware.com/support/pubs/vs_pages/vsp_pubs_esxi41_e_vc41.html

You must also have the VM environment client, such as VMware vSphere Client, installed on a management computer. (A management computer is a desktop or a laptop that you will use to deploy and manage your virtual machines.)

Downloading the FortiAuthenticator-VM software & registering with Technical Support

When purchasing FortiAuthenticator-VM from your reseller, you will receive an email that contains a registration number. This is used to download the software, your purchased license, and also to register your purchase for technical support.

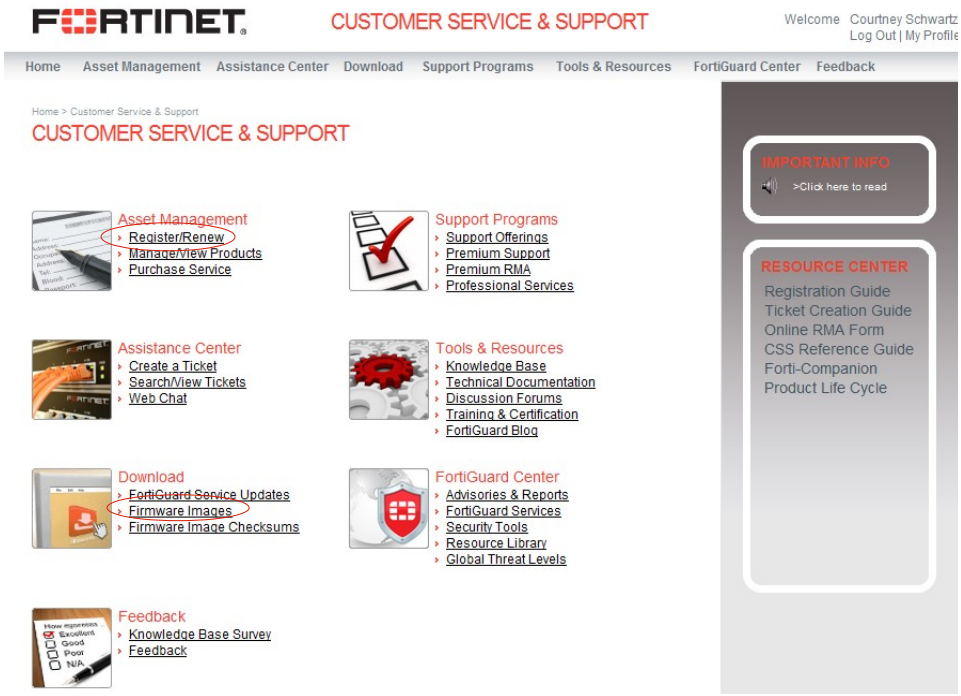
Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

To register & download FortiAuthenticator-VM and your license

1 On your management computer, start a web browser.

2 Log in to the Fortinet Technical Support web site:
https://support.fortinet.com/



3 In the *Asset Management* quadrant of the page, click *Register/Renew*.

4 Provide the registration number that was emailed to you when you purchased the

software. Registration numbers are a hyphenated mixture of 25 numbers and characters in groups of 5, such as:

`12C45-AB3DE-678G0-F9HIJ-123B5`

A registration form will appear.

5 Use the form to register your ownership of FortiAuthenticator-VM with Technical Support.

After completing the form, a registration acknowledgment page will appear.

6 Click the *License File Download* link.

Your browser will download the `.lic` file that was purchased for that registration number.

7 In the upper left corner of the page, click the *Home* link to return to the initial page.

8 In the *Download* quadrant of the page, click *Firmware Images*.

9 Click the FortiAuthenticator link and navigate to the version that you want to download.

10 Download the `.zip` file. You will use this for ***new virtual appliance (VM)*** installations. Contains a deployable virtual machine package. (`.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)

Note: Files for FortiAuthenticator-VM have a `FAC_VM` file name prefix.Other prefixes indicate that the file is for hardware versions of FortiAuthenticator such as FortiAuthenticator-3000C. Such other files cannot be used with FortiAuthenticator-VM.

11 Extract the `.zip` compressed archive's contents to a folder.

12 Continue by deploying the virtual appliance package (see Deploying FortiAuthenticator-VM on VMware vSphere).

Deploying FortiAuthenticator-VM on VMware vSphere

Installation varies slightly by virtualization platform. These instructions detail the process for installing FortiAuthenticator-VM on VMware vSphere, which is described in the subsequent text.

Deploying the OVF file

Before you can configureFortiAuthenticator-VM, you must first use VMware vSphere Client to deploy the FortiAuthenticator-VM OVF package.

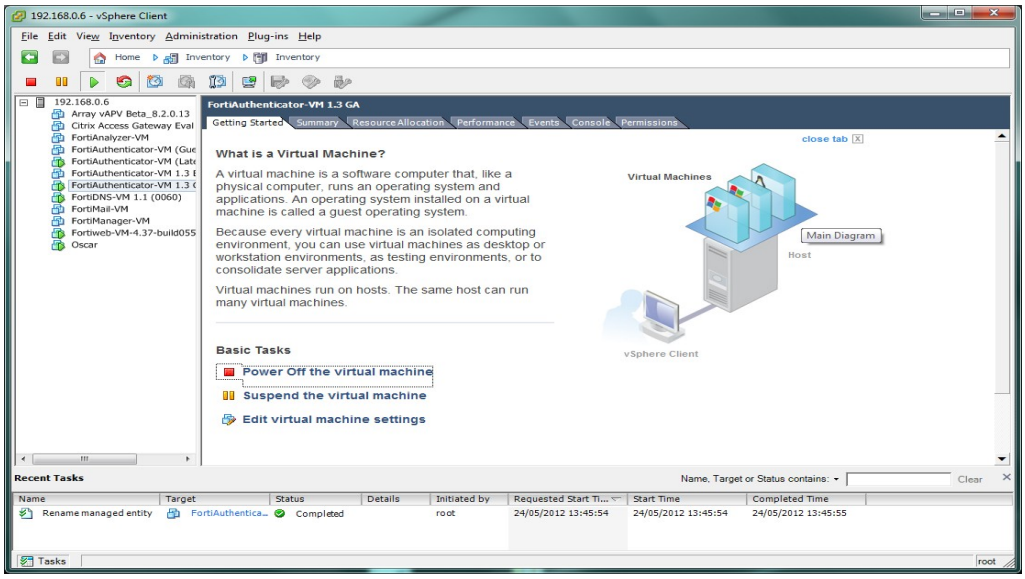
To deploy the virtual appliance

1 On your management computer, start VMware vSphere Client.

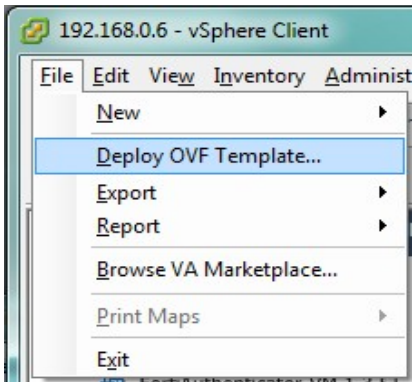
2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.

3 In *User name*, type the name of your account on that server.
4 In *Password*, type the password for your account on that server.
5 Click *Login*.

When you successfully log in, the vSphere Client window appears.

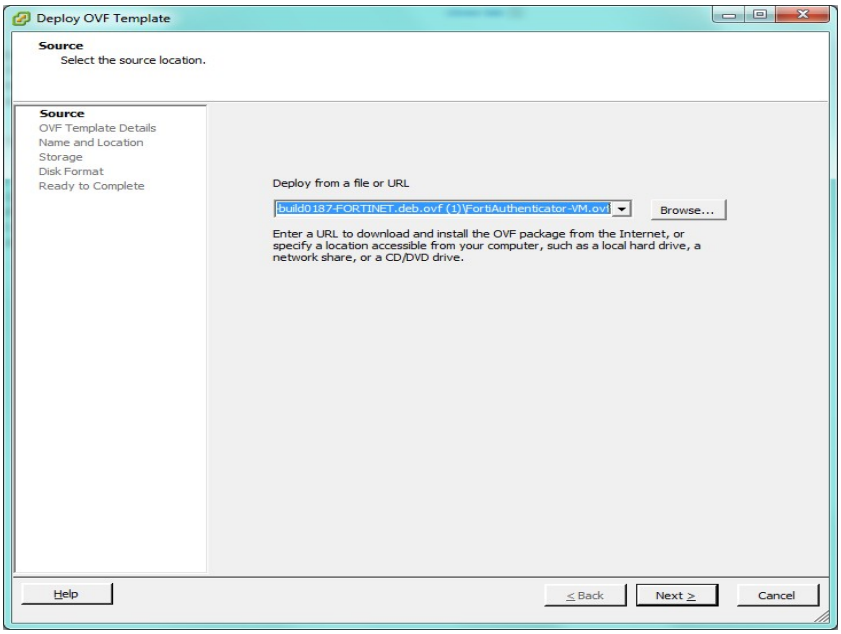


6 Go to *File* > *Deploy OVF Template.*



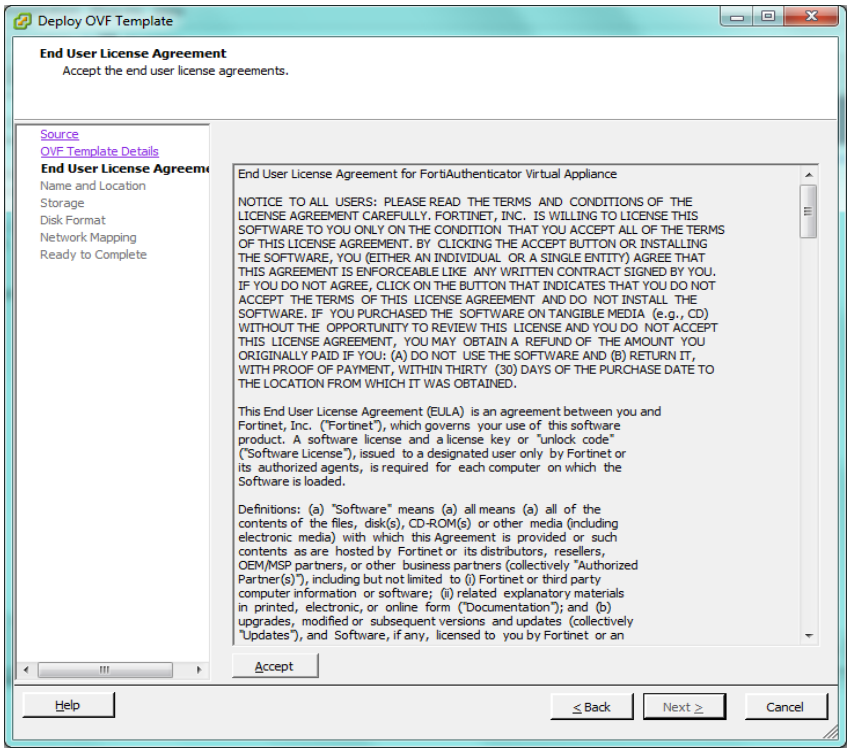
A deployment wizard window appears.

7 In the *Deploy OVF Template* window, click *Browse*, then locate the Open Virtualization Format FortiAuthenticator-VM.ovf file.



8 Click *Next* twice.

9 You will be presented with the FortiAuthenticator End User License Agreement for Virtual Appliances. Read and Accept or cancel and terminate the installation.

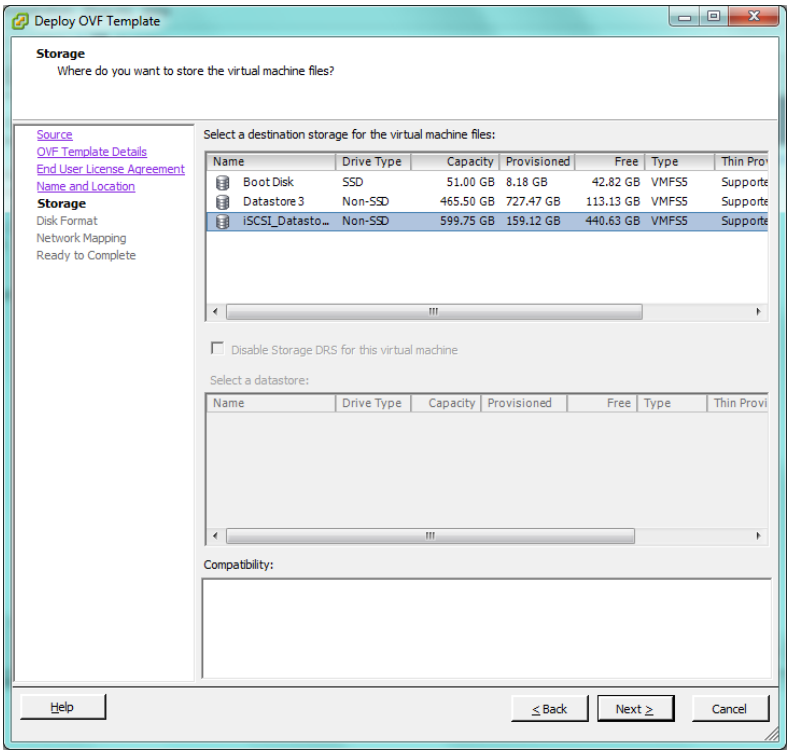


10 In *Name*, type a unique descriptive name for this instance of FortiAuthenticator-VM as it will appear in vSphere Client's inventory, such as `FortiAuthenticator-VM v1.3 GA`. If you will deploy multiple instances of this file, consider a naming scheme that will make each VM's purpose or IP address easy to remember. (This name will

not be used as the host name, nor will it appear within the FortiAuthenticator-VM web UI.)

11 Click *Next*.

12 Select the storage location in which to install the virtual machine files



13 Click *Next*

14 For the storage repository, select either:

- *Thin provisioned format* — Allocate more disk space on demand, if the storage repository uses a VMFS3 or newer file system.
- *Thick provisioned format* — Immediately allocate of disk space (specifically 32 GB) for the storage repository

Note: The best choice depends on your virtualization environment. The most optimal method is to deploy in Thick Provisioned Format because the disk space is allocated at time of the installation. Thin provisioning has the benefit of using less disk space initially. However, performance is decreased, and issues can occur the disk becomes filled with other VM instances.

15 Click *Next*.

16 If the hypervisor has more than one possible network mapping for its vSwitch, click to select the row for the network mapping that FortiAuthenticator-VM should use.

17 Click *Next*.

18 Click *Finish*.

The wizard closes. The client connects to the VM environment and deploys the OVF to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take several minutes to complete.

The vSphere Client window reappears. The navigation pane's list of virtual machines on the left now should include your new instance of FortiAuthenticator-VM (e.g. .FortiAuthenticator-VM 1.3 GA)

19 Continue with *Configuring the virtual appliance's virtual hardware settings*.

Note: Do ***not*** power on the virtual appliance ***until*** you:

- Resize the virtual disk (VMDK) (see *Resizing the virtual disk (vDisk)*)
- Set the number of vCPUs (see *Configuring the number of virtual CPUs (vCPUs)*)
- Set the vRAM on the virtual appliance (*Configuring the virtual RAM (vRAM) limit*)
- Map the virtual network adapter(s) (*Mapping the virtual NICs (vNICs) to physical NICs*).

These settings cannot be configured inside FortiAuthenticator-VM, and must be configured in the VM environment. ***Some settings cannot be reconfigured after you power on the virtual appliance.***

Configuring the virtual appliance's virtual hardware settings

After installing FortiAuthenticator-VM, log in to VMware vSphere on the server and configure the virtual appliance's hardware settings to suit the size of your deployment.

For information on the limits of configurable values for FortiAuthenticator-VM, see the *FortiAuthenticator Administration Guide*.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance's storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk ***before*** powering on.

Note: This step is not applicable if the virtual appliance will use external network file system (such as ***NFS) datastores.***

The FortiAuthenticator-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files of 1 GB for disk 1 (for the OS) and 60 GB for disk 2 data, which is large enough for most small deployments. However this can be extended if necessary. ***Resize the vDisk before powering on the virtual machine.***

Before doing so, make sure that you understand the effects of your vDisk settings.

During the creation of a VM datastore, you have the following formatting options:

- 1 MB block size - 256 GB maximum file size
- 2 MB block size - 512 GB maximum file size
- 4 MB block size – 1,024 GB maximum file size
- 8 MB block size – 2,048 GB maximum file size

These options affect the possible size of each vDisk.

For example, if you have an 800 GB datastore which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB on your FortiAuthenticator-VM.

Consider also that, depending on the size of your organization's network, you might require more or less storage for the user database and logging.

For more information on vDisk sizing, see:

http://communities.vmware.com/docs/DOC-11920

To resize the vDisk

1 On your management computer, start VMware vSphere Client.

2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.

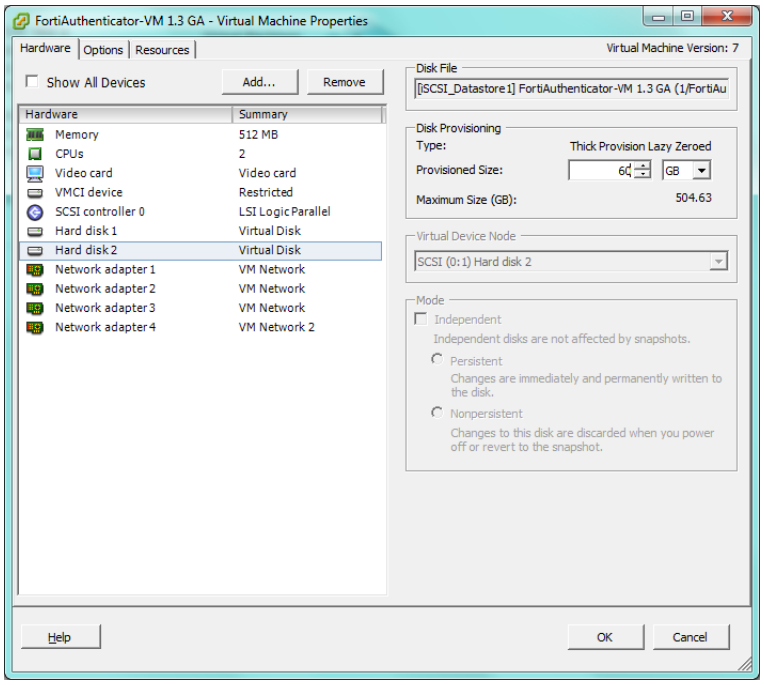
3 In *User name*, type the name of your account on that server.

4 In *Password*, type the password for your account on that server.

5 Click *Login*.

6 In the left pane, right-click the name of the virtual appliance, such as *FortiAuthenticator-VM 1.3 GA*, then select *Edit Settings*.

The virtual appliance's properties dialog appears.



7 In the list of virtual hardware on the left side of the dialog, click *Hard disk 2*.

8 Click *Remove*.

9 Click *Add*.

The *Add Hardware* dialog appears.

10 In the list of device types, click *Hard Disk*.

11 Click Next.

12 Select *Create a new virtual disk*.

13 Click *Next*.

14 In *Disk Size*, type the new size, in gigabytes (GB), of the vDisk.

15 Click *Next*.

16 Select the bottom option in *Virtual Device Node*, then from its drop-down menu, select *IDE (0:1)*.

17 Click *Next*.

18 Click *Finish*.

19 Click *OK*.

20 If you do not need to change the other resources, continue with Powering on the virtual appliance. Otherwise continue with Configuring the number of virtual CPUs (vCPUs).

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 2 vCPUs. FortiAuthenticator-VM is not restricted to how many vCPUs can be configured so you can increase the number according to your requirements e.g., you can allocate 2, 4, or 8 vCPUs.

Note: If you need to increase or decrease the vCPUs after the initial boot, power off FortiAuthenticator-VM, adjust the number of vCPUs, then see Configuring the number of virtual CPUs (vCPUs).

For more information on vCPUs, see the VMware vSphere documentation:

http://www.vmware.com/products/vsphere-hypervisor/index.html

To change the number of vCPUs

1 On your management computer, start VMware vSphere Client.

2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.

3 In *User name*, type the name of your account on that server.

4 In *Password*, type the password for your account on that server.

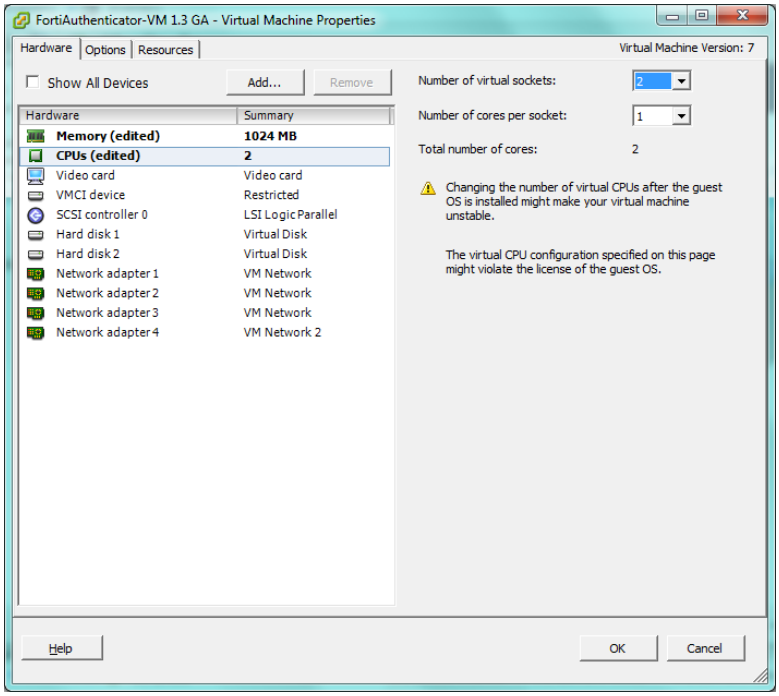
5 Click *Login*.

6 In the left pane, right-click the name of the virtual appliance, such as *FortiAuthenticator-VM 1.3 GA*, then select *Edit Settings*.

The virtual appliance's properties dialog appears.

7 In the list of virtual hardware on the left side of the dialog, click *CPUs*.

8 In *Number of virtual processors*, type the maximum number of vCPUs to allocate. Valid values range from 1 to 8.



9 Click *OK*.

10 If you do not need to change the other resources, continue with Powering on the virtual appliance. Otherwise continue with Configuring the virtual RAM (vRAM) limit.

Configuring the virtual RAM (vRAM) limit

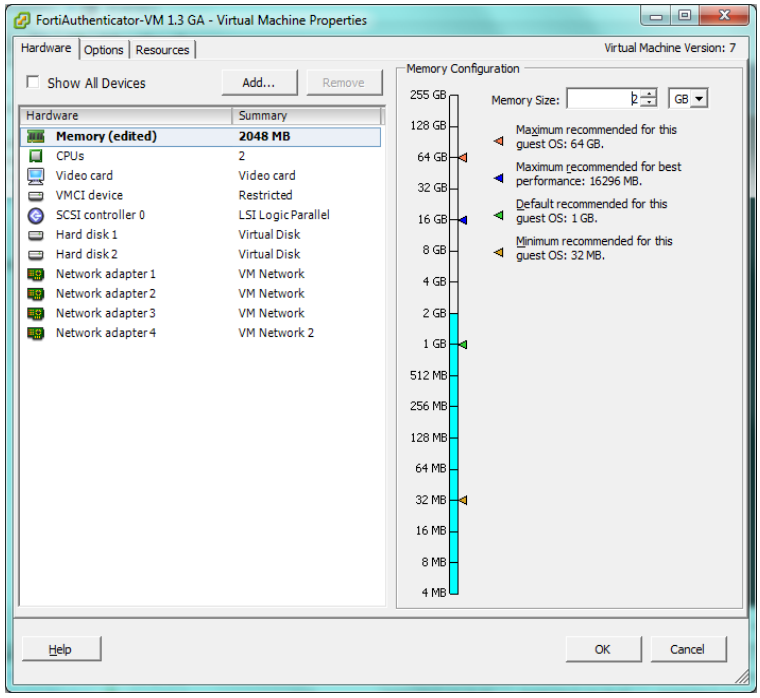
FortiAuthenticator-VM comes pre-configured to use 512 MB of vRAM. You can change this value. The valid range is from 512 MB to 16 GB.

To change the amount of vRAM

1 On your management computer, start VMware vSphere Client.
2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
3 In *User name*, type the name of your account on that server.
4 In *Password*, type the password for your account on that server.
5 Click *Login*.
6 In the left pane, right-click the name of the virtual appliance, such as *FortiAuthenticator-VM-64-101*, then select *Edit Settings*.

The virtual appliance's properties dialog appears.

7 In the list of virtual hardware on the left side of the dialog, click *Memory*.
8 In *Memory Size*, type the maximum number in gigabytes (GB) of the vRAM to allocate. Valid values range from 2 to 4.



9 Click *OK*.
10 If you do not need to change the other resources, continue with Powering on the virtual appliance. Otherwise continue with Mapping the virtual NICs (vNICs) to physical NICs.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiAuthenticator-VM ports to physical ports depends on your existing virtual environment.

Note: Often, the default bridging vNICs work, and don't need to be changed.

If you are unsure of your network mappings, try bridging first ***before*** non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines should have their own IP addresses on your network.

The most common exceptions to this rule are for VLANs and the transparent modes. See Mapping the virtual NICs (vNICs) to physical NICs.

When you deploy the FortiAuthenticator-VM package, 4 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 4 network interfaces in FortiAuthenticator-VM. (Alternatively, if you prefer, some or all of the network interfaces may be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

Example: Network mapping

VMware vSphere			FortiAuthenticator-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiAuthenticator-VM**	**Network Interface Name in Web UI/CLI**
eth0	VM Network 0	Management	port1
eth1	VM Network 1	External	port2
eth0	VM Network 2	Internal (LDAP)	port3
eth0	VM Network 1	Unconfigured	port4

To map network adapters

1 On your management computer, start VMware vSphere Client.

2 Enter the IP address, user name, and password of the VMware vSphere server.

3 Click *Login*.

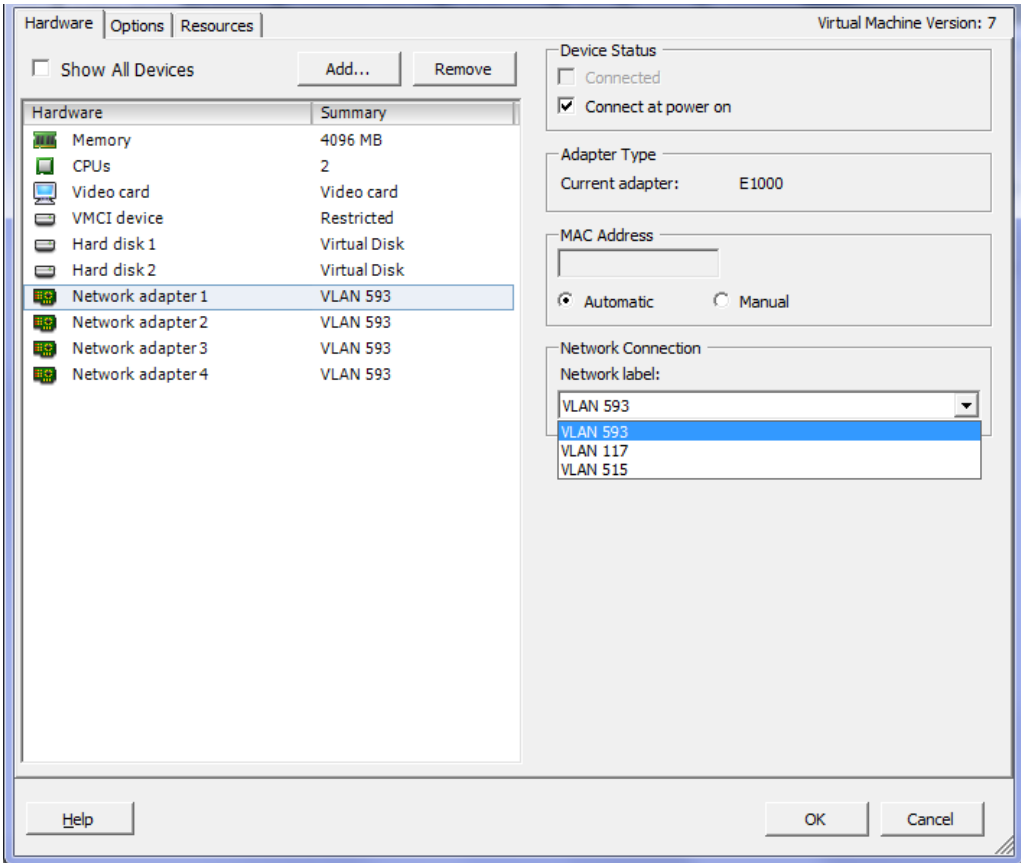
4 In the left pane, right-click the name of the virtual appliance, such as *FortiAuthenticator-VM 1.3 GA*, then select *Edit Settings*.

The virtual appliance's properties dialog appears.

5 In the list of virtual hardware on the left side of the dialog, click the name of a virtual network adapter to see its current settings.

6 From the *Network Connection* drop-down menu, select the virtual network mapping for the virtual network adapter.

The correct mapping varies by your virtual environment's network configuration. In the example illustration below, the vNIC *Network adapter 1* is mapped to the virtual network (vNetwork) named *VLAN 593.*



7 Click *OK*.

8 Continue with Powering on the virtual appliance.

Powering on the virtual appliance

Once the virtual appliance's package has been deployed and its virtual hardware configured, you can power on the virtual appliance.

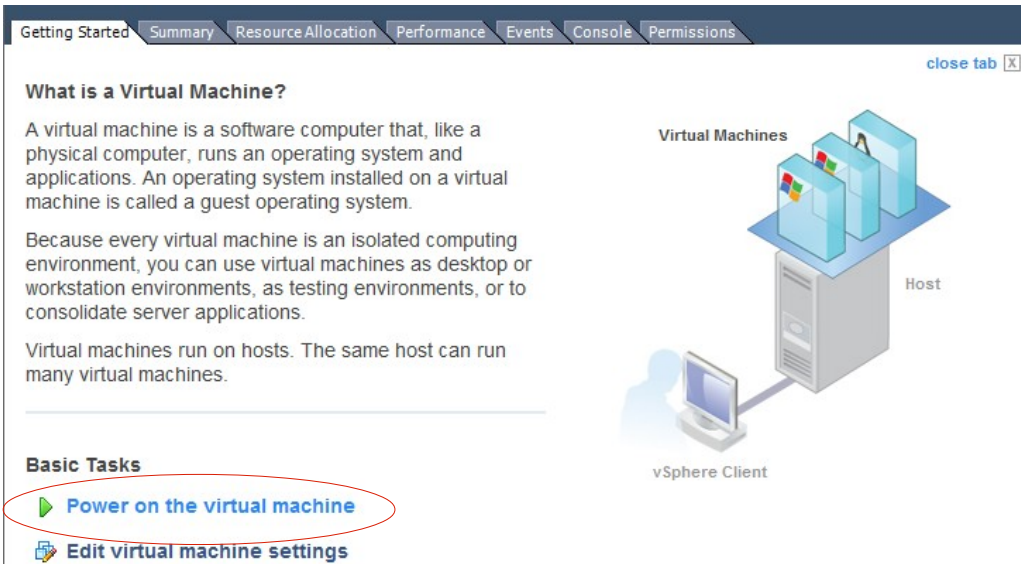
Note: Do ***not*** power on the virtual appliance ***unless*** you have already mapped the virtual network adapter(s) (Mapping the virtual NICs (vNICs) to physical NICs). You may also want to:

- Resize disk (VMDK) (see Resizing the virtual disk (vDisk))
- Configure the number of CPUs (see Configuring the number of virtual CPUs (vCPUs))
- Set the RAM on virtual appliance (Configuring the virtual RAM (vRAM) limit)

These settings cannot be configured inside FortiAuthenticator-VM, and must be configured in the virtual machine environment.

To power on FortiAuthenticator-VM

1 On your management computer, start VMware vSphere Client.
2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
3 In *User name*, type the name of your account on that server.
4 In *Password*, type the password for your account on that server.
5 Click *Login*.
6 In the left pane, click the name of the virtual appliance, such as *FortiAuthenticator-VM 1.3 GA*.
7 Click the *Getting Started* tab.



8 Click *Power on the virtual machine*.
9 Continue with Configuring access to the web UI & CLI

Configuring access to the web UI & CLI

Once it is powered on, you must log in to the FortiAuthenticator-VM command line interface (CLI) via the console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings in FortiAuthenticator-VM

1 On your management computer, start VMware vSphere Client.

2 Log in to the VM environment.

3 Open the console of the FortiAuthenticator-VM virtual appliance.

On VMware vSphere Client:

- In the left pane, select the name of the virtual appliance, such as *FortiAuthenticator-VM 1.3 GA*.
- Click the *Console* tab.

4 At the login prompt for the local console, type:

```
admin
```

5 Press Enter twice. (Initially, there is no password.)

By default the IP of `Port1` is set to `192.168.1.99/24`. If you need to change this. You can configure the IP address and netmask of the network interface . Type:

```
set port1-ip <address_ipv4> <netmask_ipv4>
```

where:

`<address_ipv4>` is the IP address assigned to the network interface, such as `192.168.1.99`; the correct IP will vary by your configuration of the vNetwork (see Mapping the virtual NICs (vNICs) to physical NICs)

`<netmask_ipv4>` is its netmask in dotted decimal format, such as `255.255.255.0`

6 Configure a static route with the default gateway. Type:

```
set default-gw <router_ipv4>
```

where `<router_ipv4>` is the IP address of the gateway router.

You should now be able to connect via the network from your management computer to `port1` of FortiAuthenticator-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to https://192.168.1.1/)
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22.) Note that there is minimal configuration available via SSH. The primary location for configuration is via the GUI (HTTPS).

7 Continue by uploading the license file (see Uploading the license).

Note: The built in 2-user license allows you to test features. A full evaluation license is available on request.

You can upgrade to an evaluation on permanent license at any time by uploading the license file via *System* > *Maintenance* > *License* option in the *System Information* widget in the system dashboard of the web UI. For instructions, see Uploading the license.

Uploading the license

When you purchase a license for FortiAuthenticator-VM, you will be provided with a license serial number which can be entered into the Fortinet support site to generate a license key.

You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

Note: As your organization grows, you can simply either allocate more resources or migrate your virtual appliance to a physical server with more power, then upgrade your FortiAuthenticator-VM license to support your needs.

To upload the license via the web UI

1 On your management computer, start a web browser.

Your computer must be connected to the same network as the hypervisor or be able to route to it and have HTTPS access.

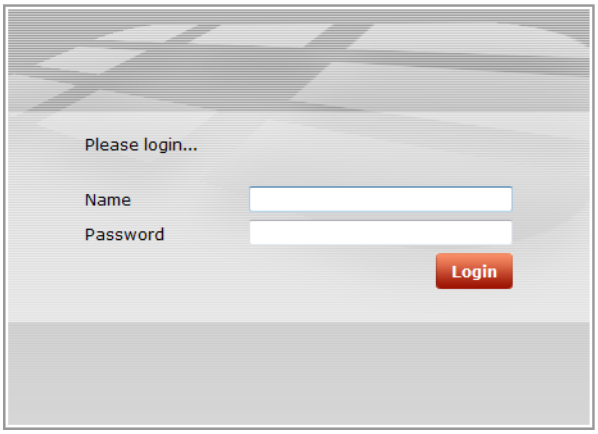
2 In your browser's URL or location field, enter the IP address of `port1` of the virtual appliance, such as:

https://192.168.1.99/ or the IP address you have changed the management interface to.

(Remember to include the "s" in https://.)

Note: Initially, you must access the web UI via HTTPS. By default, HTTP is not enabled. After uploading the license, you can configure the administrative access protocols. For details, see the *FortiAuthenticator Administration Guide*.

Your browser connects the appliance. The web UI's login page should appear.



To support HTTPS authentication, the FortiAuthenticator appliance ships with a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiAuthenticator appliance. When you connect, depending on your web browser and prior access of the FortiAuthenticator appliance, your browser might display two security warnings related to this certificate:

- The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
- The certificate might belong to another web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether thismismatch is normal or not.

Both warnings are normal for the default certificate. SSL v3 and TLS v1.0 are supported.

3 Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate.

For details on accepting the certificate, see the documentation for your web browser.

4 In the *Name* field, type `admin`.

5 Click *Login*. (Initially, there is no password.)

The web UI appears.The web UI initially displays its dashboard, *System* > *Status* > *Status*. The *FortiGuard Information* widget displays the current license status and contains a link where you can upload a license file.

6 In the *VM License* row of the *FortiGuard Information* widget, click the *Update* link.

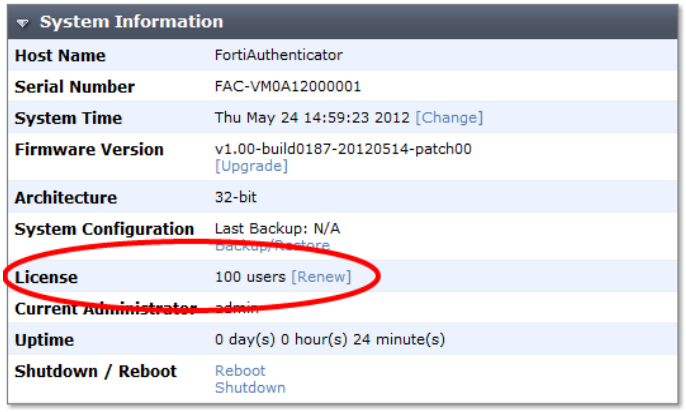
The *Install FortiAuthenticator-VM License File* dialog opens.Depending on your browser, you may see either a *Browse* or *Choose File* button. Locate the license file (.lic) you downloaded earlier from Fortinet, then click *OK*.

Your browser uploads the license file. Time required varies by the size of the file and the speed of the network connection. FortiAuthenticator will then connect to Fortinet to validate its license. A message appears:

```
License has been uploaded successfully.
```

7 Click *OK*

8 To verify that the license was uploaded successfully, the license section of the System Information Widget in the Status Dashboard should display the licensed number of users e.g. 100 as in the example below.



9 Continue with What's next?.

What's next?

At this point, the FortiAuthenticator-VM virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. Before you can use FortiAuthenticator-VM, you must configure it.

Configure the FortiAuthenticator-VM software using the FortiAuthenticator Administration Guide.

After you have completed this first-time setup, you can refer to the *FortiAuthenticator Administration Guide*. Updates, reconfiguration, and ongoing use of both FortiAuthenticator-VM virtual appliances and physical appliance models such as FortiAuthenticator-400C are the same.

Updating the virtual hardware

By default, FortiAuthenticator-VM uses VMware virtual hardware version 5. Should you need to update your FortiAuthenticator-VM's virtual hardware, simply be sure to shut down FortiAuthenticator-VM before doing so.

For example, if you have a VMware ESX 4.0 environment that supports virtual hardware version 7, and you want to provide version 7 feature support such as backups to FortiAuthenticator-VM, you would update the virtual hardware.

For more information on virtual hardware, see:

http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675

To update the virtual hardware

1 Shut down FortiAuthenticator-VM. To do this, you can enter the CLI command:

```
execute shutdown
```

2 In VMware vCenter, right-click the VM and select the option to upgrade the virtual hardware.

3 When the upgrade is complete, power on FortiAuthenticator-VM.

Appendix A – Maximum Values

The main criteria for licensing the FortiAuthenticator is the number of users it supports. Other metrics are limited in line with this figure. Some of these metrics are hard coded relative to the capabilities of the hardware. With FortiAuthenticator-VM, because of the stackable nature of the license, the limits are relative to the number of users licensed.

Feature	Unlicensed VM	Licensed VM (example max users: 100)	FortiAuthenticator 400C	FortiAuthenticator 1000C	FortiAuthenticator 3000B
Users	2	100	2000	10000	20000
Fortitokens	10	200 (Num of users x 2)	2000	10000	20000
User Groups	3	10 (Num of users / 10)	50	200	2000
Remote Groups (SSO Groups)	30	50 (Num of users / 2)	1000	5000	10000
User Radius Attributes	6	300 (Num of users x 3)	6000	30000	60000
Group Radius Attributes	9	300 (Num of user groups x 3)	150	600	6000
Device (MAC-based Auth.)	1	10 (Num of users / 10)	200	1000	2000
Remote LDAP Users	10	100 (Same as num of users)	2000	10000	20000
NAS	3	10 (Num of users / 10)	200	1000	2000
LDAP Entries	20	200 (Num of users x 2)	1000	4000	40000
Remote LDAP Servers	3	20	20	20	20
FSAE Domain Controllers	3	20	20	20	20
CA Certificates	3	5 (Num of users / 20)	10	50	250
Trusted CA Certificates	5	200	200	200	200
User Certificates	5	100 (Same as num of users)	500	2000	20000
SMTP Servers	3	20	20	20	20

FortiAuthenticator-VM 1.0 MR3 Install Guide

May 29, 2012 • 1st Edition

Technical Documentation	http://docs.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	http://support.fortinet.com/forum
Training	http://training.fortinet.com
Technical Support	https://support.fortinet.com

Please report errors or omissions to:
techdoc@fortinet.com